HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 821 Pub. Rec and Meetings/Information Technology Security Information
SPONSOR(S): Oversight, Transparency & Public Management Subcommittee; Williamson and others
TIED BILLS: **IDEN./SIM. BILLS:** SB 1170

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Oversight, Transparency & Public Management Subcommittee	13 Y, 0 N, As CS	Toliver	Smith
2) State Affairs Committee			

SUMMARY ANALYSIS

The Information Technology (IT) Security Act requires the Department of Management Services (DMS) and state agency heads to meet certain requirements in order to secure and protect state IT resources and the information contained therein. Currently, the IT Security Act provides public record exemptions for:

- Portions of risk assessments, evaluations, external audits, and other reports of a state agency's IT security program for the data, information, and IT resources of the state agency if disclosure would facilitate the unauthorized access to, or the unauthorized modification, disclosure, or destruction of data or IT resources;
- Internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources;
- The results of internal audits and evaluations; and
- Records which identify detection, investigation, or response practices for suspected or confirmed IT security incidents.

The bill expands the current public record exemption for records which identify detection, investigation, or response practices of IT security incidents in the IT security act to include network schematics, hardware and software configurations, or encryption. The bill also creates a public meeting exemption in the IT security act for those portions of a public meeting which would reveal any of the following confidential and exempt records:

- Portions of records which contain network schematics, hardware or software configurations, or encryption;
- Portions of records which identify detection, investigation, or response practices for suspected or confirmed IT security incidents; and
- Portions of risk assessments, evaluations, external audits, and other reports of a state agency's IT security program for the data, information, and IT resources of the state agency if disclosure would facilitate the unauthorized access to, or the unauthorized modification, disclosure, or destruction of data or IT resources.

Any portion of a meeting exempt under the bill must be recorded and transcribed and those recordings and transcripts are confidential and exempt from public record requirements unless a court of competent jurisdiction, determines that the meeting was not restricted to the discussion of data and information. The bill provides for retroactive application of the public record and public meeting exemptions. It also provides for repeal of the exemptions on October 2, 2025, unless reviewed and saved from repeal through reenactment by the Legislature. Lastly, the bill provides a public necessity statement as required by the Florida Constitution.

Article I, s. 24(c) of the Florida Constitution requires a two-thirds vote of the members present and voting for final passage of a newly created or expanded public record or public meeting exemption. The bill expands a public record exemption for certain records relating to IT security and creates a public meeting exemption; thus, it requires a two-thirds vote for final passage.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Public Records

Article I, s. 24(a) of the State Constitution sets forth the state's public policy regarding access to government records. This section guarantees every person a right to inspect or copy any public record of the legislative, executive, and judicial branches of government. The Legislature, however, may provide by general law for the exemption of records from the requirements of Article I, section 24(a).[1] The general law must state with specificity the public necessity justifying the exemption and must be no more broad than necessary to accomplish its purpose.[2]

Public policy regarding access to government records is addressed further in the Florida Statutes. Section 119.07(1), F.S., guarantees every person a right to inspect and copy any state, county, or municipal record. Furthermore, the Open Government Sunset Review Act[3] provides that a public record or public meeting exemption may be created or maintained only if it serves an identifiable public purpose. In addition, it may be no broader than is necessary to meet one of the following purposes:

- Allow the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption.
- Protect sensitive personal information that, if released, would be defamatory or would jeopardize an individual's safety; however, only the identity of an individual may be exempted under this provision.
- Protect trade or business secrets.[4]

The Open Government Sunset Review Act requires the automatic repeal of a newly created exemption on October 2nd of the fifth year after creation or substantial amendment, unless the Legislature reenacts the exemption.[5]

Public Meetings

Article I, s. 24(b) of the State Constitution sets forth the state's public policy regarding access to government meetings. It requires all meetings of any collegial public body of the executive branch of state government or of any collegial public body of a county, municipality, school district, or special district, at which official acts are to be taken or at which public business of such body is to be transacted or discussed, to be noticed and open to the public.

Public policy regarding access to government meetings is also addressed in the Florida Statutes. Section 286.011, F.S., known as the "Government in the Sunshine Law" or "Sunshine Law," further requires all meetings of any board or commission of any state agency or authority or of any agency or authority of any county, municipal corporation, or political subdivision at which official acts are to be taken to be open to the public at all times. The board or commission must provide reasonable notice of all public meetings.[6] Minutes of a public meeting must be promptly recorded and be open to public inspection.[7] No resolution, rule, or formal action is considered binding, unless action is taken or made at a public meeting.[8]

[1] Art. I, s. 24(c), FLA. CONST.
[2] *Id.*
[3] Section 119.15, F.S.
[4] Section 119.15(6)(b), F.S.
[5] Section 119.15(3), F.S.
[6] Section 286.011(1), F.S.
[7] Section 286.011(2), F.S.
[8] Section 286.011(1), F.S.

Information Technology Security Act

The Information Technology (IT) Security Act[9] requires the Department of Management Services (DMS) and the heads of state agencies[10] to meet certain requirements to enhance the IT[11] security of state agencies. Specifically, the IT Security Act provides that DMS is responsible for establishing standards and processes consistent with generally accepted best practices for IT security,[12] including cybersecurity, and adopting rules that safeguard an agency's data, information, and IT resources to ensure availability, confidentiality, and integrity and to mitigate risks.[13] In addition, DMS must:

- Designate a state chief information security officer;
- Develop, and annually update, a statewide IT security strategic plan;
- Develop and publish an IT security framework for state agencies;
- Collaborate with the Cybercrime Office within the Florida Department of Law Enforcement (FDLE) in providing training for state agency information security managers; and
- Annually review the strategic and operational IT security plans of executive branch agencies.[14]

The IT Security Act requires the head of each state agency to designate an information security manager to administer the IT security program of the state agency.[15] In addition, the head of each state agency must annually submit to DMS the state agency's strategic and operational IT security plans; conduct, and update every three years, a comprehensive risk assessment to determine the security threats to the data, information, and IT resources of the state agency; develop, and periodically update, written internal policies and procedures, including procedures for reporting IT security incidents and breaches; and ensure that periodic internal audits and evaluations of the agency's IT security program for the data, information, and IT resources are conducted.[16]

Current Public Record Exemptions under the IT Security Act

Currently, the IT Security Act provides that the following state agency information is confidential and exempt[17] from public record requirements:

- Comprehensive risk assessments;[18]
- Portions of risk assessments, evaluations, external audits,[19] and other reports of a state agency's IT security program for the data, information, and IT resources of the state agency if disclosure would facilitate the unauthorized access to, or the unauthorized modification, disclosure, or destruction of:
    - Physical or virtual data or information; or

[9] Section 282.318, F.S.

[10] The term "state agency" is defined to mean any official, officer, commission, board, authority, council, committee, or department of the executive branch of state government; the Justice Administrative Commission; and the Public Service Commission. The term does not include university boards of trustees or state universities. Section 282.0041(27), F.S. For purposes of the IT security act, the term includes the Department of Legal Affairs, the Department of Agriculture and Consumer Services, and the Department of Financial Services. Section 282.318(2), F.S.

[11] The term "information technology" is defined to mean equipment, hardware, software, firmware, programs, systems, networks, infrastructure, media, and related material used to automatically, electronically, and wirelessly collect, receive, access, transmit, display, store, record, retrieve, analyze, evaluate, process, classify, manipulate, manage, assimilate, control, communicate, exchange, convert, converge, interface, switch, or disseminate information of any kind or form. Section 282.0041(14), F.S.

[12] The term "information technology security" is defined to mean the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of data, information, and information technology resources. Section 282.0041(17), F.S.

[13] Section 282.318(3), F.S.

[14] *Id.*

[15] Section 282.318(4)(a), F.S.

[16] Section 282.318(4), F.S.

[17] There is a difference between records the Legislature designates exempt from public records requirements and those the Legislature deems confidential and exempt. A record classified as exempt from public disclosure may be disclosed under certain circumstances. *See Williams v. City of Minneola*, 575 So. 2d 683, 687 (Fla. 5th DCA 1991) *review denied*, 589 So. 2d 289 (Fla. 1991). If the Legislature designates a record as confidential and exempt from public disclosure, such record may not be released by the custodian of public records to anyone other than the persons or entities specifically designated in statute. *See WFTV, Inc. v. Sch. Bd. of Seminole Cnty*, 874 So. 2d 48, 53-54 (Fla. 5th DCA 2004), *review denied*, 892 So. 2d 1015 (Fla. 2004); Op. Att'y Gen. Fla. 85-62 (1985).

[18] Section 282.318(4)(d), F.S.

[19] The term "external audit" is defined to mean an audit that is conducted by an entity other than the state agency that is the subject of the audit. Section 282.318(5), F.S.

    - IT resources, including information relating to the security of the state agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or physical or virtual security information that relates to the state agency's existing or proposed IT systems.[20]
- Internal policies and procedures that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources;[21]
- The results of internal audits and evaluations;[22] and
- Records which identify detection, investigation, or response practices for suspected or confirmed IT security incidents.[23]

The confidential and exempt information must be disclosed to the Auditor General, the Cybercrime Office within FDLE, the Division of State Technology[24] within DMS, and, for agencies under the jurisdiction of the Governor, the Chief Inspector General.[25]

Effect of the Bill

The bill expands the current public exemption for records which identify detection, investigation, or response practices of IT security incidents in the IT Security Act to include network schematics, hardware and software configurations, or encryption. The records would be confidential and exempt from public records requirements and would only be available to the Auditor General, the Cybercrime Office within FDLE, the Division of State Technology within DMS, and for agencies under the jurisdiction of the Governor, the Chief Inspector General.

The bill also creates a public meeting exemption in the IT Security Act for those portions of a public meeting which would reveal any of the following confidential and exempt records:

- Portions of records which contain network schematics, hardware or software configurations, or encryption;
- Portions of records which identify detection, investigation, or response practices for suspected or confirmed IT security incidents;
- Portions of risk assessments, evaluations, external audits, and other reports of a state agency's IT security program for the data, information, and IT resources of the state agency if disclosure would facilitate the unauthorized access to, or the unauthorized modification, disclosure, or destruction of:
    - Physical or virtual data or information; or
    - IT resources, including information relating to the security of the state agency's technologies, processes, and practices designed to protect networks, computers, data processing software, and data from attack, damage, or unauthorized access; or physical or virtual security information that relates to the state agency's existing or proposed IT systems.

Any portion of a meeting exempt under the bill must be recorded and transcribed. The recordings and transcripts are confidential and exempt from public record requirements unless a court of competent jurisdiction, following an in camera review, determines that the meeting was not restricted to the discussion of data and information. If such a judicial determination occurs, only the portion of the recording or transcript which reveals nonexempt data may be disclosed to a third party.

The bill provides for retroactive application of the public record and public meeting exemptions. It also provides for repeal of the exemptions on October 2, 2025, unless reviewed and saved from repeal

[20] Section 282.318(5)., F.S.
[21] Section 282.318(4)(e), F.S.
[22] Section 282.318(4)(g), F.S.
[23] Section 282.318(4)(j)3., F.S.
[24] The Division of State Technology (formerly the Agency for State Technology) is a contained within DMS and is charged with overseeing the state's IT resources. Section 20.22(2)(b), F.S,
[25] Sections 282.318(4)(d),(e), (g), (j) and 282.318(5), F.S.

through reenactment by the Legislature. Finally, the bill provides a public necessity statement as required by the Florida Constitution.

B. SECTION DIRECTORY:

Section 1 amends s. 282.318, F.S., relating to the IT Security Act.

Section 2 provides a public necessity statement.

Section 3 provides an effective date of upon becoming a law.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

The bill could have a minimal fiscal impact on state agencies because staff responsible for complying with public records requests may require training related to creation of the public record exemptions. In addition, agencies could incur costs associated with redacting the confidential and exempt records prior to release. The costs, however, would be absorbed, as they are part of the day-to-day responsibilities of state agencies.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. This bill does not appear to affect county or municipal governments.

2. Other:

Article I, section 24(c) of the Florida Constitution requires a two-thirds vote of the members present and voting for final passage of a newly created or expanded public record or public meeting exemption. The bill expands a public record exemption and creates a public meeting exemption; therefore, it requires a two-thirds vote for final passage.

Public Necessity Statement

Article I, section 24(c) of the Florida Constitution requires a public necessity statement for a newly created or expanded public record or public meeting exemption. The bill expands a public record exemption and creates a public meeting exemption; therefore, it includes a public necessity statement.

Breadth of Exemption

Article I, section 24(c) of the Florida Constitution requires a newly created public record or public meeting exemption to be no broader than necessary to accomplish the stated purpose of the law. The bill creates public record exemptions for certain state agency records, and portions thereof, related to IT security. The release of such records could result in the identification of vulnerabilities or gaps in a state agency's IT security system or processes and thereby increase the risk of an IT security incident or breach. Thus, the bill does not appear to be in conflict with the constitutional requirement that an exemption be no broader than necessary to accomplish its purpose.

B. RULE-MAKING AUTHORITY:

The bill does not confer rulemaking authority on an agency nor does it require the promulgation of rules.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On January 16, 2020, the Oversight, Transparency & Public Management Subcommittee adopted an amendment and reported the bill favorably as a committee substitute. The amendment was technical in nature and moved the definition of "external audit," which applied to the entire subsection, from a subparagraph to the subsection as a whole.

This analysis is drafted to the committee substitute as adopted by the Oversight, Transparency & Public Management Subcommittee.